



# State of Nevada

## State Information Technology Security Committee

### Standard

Control No.	Rev.	Title	Effective Date	Page
4.07	A	IT Contingency Planning	04/11/02	1 of 3

#### 1.0 PURPOSE

This standard establishes the minimum Information Technology (IT) Contingency Planning standard for an agency's mission critical information and the IT resources that support the critical mission of the agency.

Each agency must be able to continue to provide mission-critical services that are supported by IT resources should a situation occur that renders the IT resources inaccessible due to a system or application malfunction or hardware failure.

For the purpose of this policy "contingency planning" includes, but is not limited to, the documentation, plans, and policies and procedures required to restore mission-critical IT functions to include mainframe, mini-computers, servers, microcomputers, voice and data communications services, applications systems and related data.

#### 2.0 SCOPE

This standard applies to all state agencies meeting the requirements identified in the State IT Security Policy, Section 2.0 Scope.

#### 3.0 EFFECTIVE DATES

The requirements of this standard are effective 90 days after sign-off by the Governor or his designee.

#### 4.0 RESPONSIBILITIES

The agency head or appointed agency Information Security Officer (ISO) has the responsibility to implement this standard and ensure compliance.

#### 5.0 RELATED DOCUMENTS

State IT Security Policy, 4.02  
State Information Security Officer (ISO) Roles and Responsibilities, 4.03  
National Institute of Standards and Technology (NIST) Special Publication 800-34 , Contingency Planning for Information Technology Systems, dated January 15, 2002

#### 6.0 STANDARD

A. Each agency shall develop, maintain and test IT Contingency Plans.



# State of Nevada

## State Information Technology Security Committee

### Standard

Control No.	Rev.	Title	Effective Date	Page
4.07	A	IT Contingency Planning	04/11/02	2 of 3

- B. IT Contingency Plans shall contain sufficient information and instruction to enable the agency management to assure the agency's ability to continue its critical business services and operations, including those used by branch or remote offices.
- C. Agencies that use computer or telecommunication services from other governmental entities or commercial sources shall integrate and coordinate IT Contingency Plans, including off-site storage of data.
- D. Agencies shall update IT Contingency Plans at least annually and/or following any significant change to the computing or telecommunications environment or critical function needs. Directors or identified agency heads shall review and approve agency new and revised plans.
- E. Agencies shall identify and train appropriate employees to execute the IT Contingency Plans to include making employees aware of the need, existence of the agency IT Contingency Plan, along with the employees' responsibilities, and training the recovery team members to perform the procedures defined in the plan.
- F. Agencies shall test the IT Contingency Plans and document the results. The type and extent of testing shall be dependent on the criticality of the function being supported by the IT resources. Agencies shall correct or establish a mitigation plan for correcting any deficiencies revealed by the test. The test results and mitigation plan shall be reviewed and approved by the agency head and provided to the State IT Security Committee Chair no later than January 15 of each year.

#### 7.0 DEFINITIONS/BACKGROUND

Contingency Plans are related to, but do not take the place of, other types of plans. These plans are listed below, with the differences between plans addressed:

**RISK MANAGEMENT PLAN/STRATEGY:** A Risk Management Plan identifies risks facing an agency and plans to mitigate those risks. Contingency Plans for IT resources are one component of an agency's risk strategy and thus should be consistent with the philosophy and goals of the overall risk management plan. However, Contingency Plans for IT resources are narrower in scope, dealing only with IT resources. An agency risk strategy is broader in scope, including abatements for risks in all resource categories such as staff, facilities, etc.

**DISASTER RECOVERY PLANS:** A Disaster Recovery Plan covers procedures for resuming agency functions in the case of a catastrophe. This type of planning assumes that few or none of the agency's normal operations can function. Contingency planning is similar to disaster planning, with two major differences. First, contingency planning does not assume the source of the failure, only the steps needed to resume normal operations. Secondly, contingency plans do not preclude the use of agency resources (e.g., facilities) that may not be available in the case of a true disaster.



# State of Nevada

## State Information Technology Security Committee

### Standard

Control No.	Rev.	Title	Effective Date	Page
4.07	A	IT Contingency Planning	04/11/02	3 of 3

**BUSINESS RESUMPTION PLANS:** A Business Resumption Plan covers the procedures needed to bring the agency back to normal business operations following a major disaster or business interruption. Contingency Plans address the recovery and resumption to normal operations of critical functions of the agency supported by IT resources. Whereas, a Business Resumption Plan addresses the resumption of business for the entire agency to include facilities, staff, etc.

**MITIGATION PLANS:** A Mitigation Plan describes what corrective measures need to be taken as a result of testing the contingency plan, the actions required to correct the weaknesses and a schedule to accomplish the corrective actions to include resource requirements.

#### 8.0 EXCEPTIONS/OTHER ISSUES

Requests for exception to the requirements of this IT Security Standard must be documented, provided to and approved by the State IT Security Committee and Chief Information Officer (CIO).

<i>Approved By</i>		
Title	Signature	Date
<b>State IT Security Committee Chair</b>	Signature on File	11/28/2001
<b>NV IT Operations Committee Chair</b>	Signature on File	04/11/2002
<b>Governor/Governor's Representative</b>	Signature on File	06/17/2003

<i>Document History</i>		
Revision	Date	Change
A	04/11/02	Initial release.